UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/005,271	12/05/2001	Geoffrey S. Strongin	2000.055700	6634

23720 7590 03/25/2004

WILLIAMS, MORGAN & AMERSON, P.C.
10333 RICHMOND, SUITE 1100
HOUSTON, TX 77042

EXAMINER
DINH, NGOC V

ART UNIT	PAPER NUMBER
2187	6

DATE MAILED: 03/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/005,271	**Applicant(s)** STRONGIN ET AL.	
	Examiner NGOC V DINH	**Art Unit** 2187	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _03_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _09 January 2004_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-49_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-49_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

1. This Office Action is responsive to Amendment filed 01/09/04.

Applicant's previous arguments are moot with regard to claims 1-49 in view of the new rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-3, 5-22, 24-28, 30-49 are rejected under 35 U.S.C.102 (e) as being anticipated by Christie PN 6,516,395.

2.As per claim 1:

Christie teaches a memory management unit for managing a memory storing data arranged within a plurality of memory pages [fig. 1-2], the memory management unit comprising: a security check unit [304, fig. 3B] coupled to receive a physical address within a selected memory page and security attributes of the selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure [x86, privilege level; fig. 3B; user/supervisory mode; abstract] located in the memory to obtain an additional security attribute [fig. 4; access attributes, read/write limitations, col. 13, lines 35-40; col. 15, lines 29-50] of the selected memory page, and to generate a fault signal [304, fig. 3B; col. 14, line 60 to col. 15, line 5] dependent upon the security attributes of selected memory page and the additional security attribute of the selected memory page [abstract; col. 2, lines 27-40; col. 13, lines 20-60].

3. As per claims 2, 5-10:

Christie teaches the memory management unit, wherein:

the security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=O indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=O indicates only read accesses are allowed to the selected memory page, and wherein R/W=l indicates that both read and write accesses are allowed to the selected memory page;

the at least one security attribute data structure comprises a security attribute table directory [privilege level; fig. 3B; user/supervisory mode] and at least one security attribute table [access attributes, read/write limitations; access check circuit, 402, fig. 4, col. 30-40] [fig. 3A, col. 13, lines 20-60; col. 14, lines 20-25];

the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes a secure page (SP) bit, and wherein the SP bit indicates whether or not a corresponding memory page is a secure page; the additional security attribute of the selected memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the selected memory page is a secure page [col. 13, lines 40-60; col. 14, lines 20-25];

the linear address [col. 11, lines 60-67] is produced during execution of an instruction residing within a first memory page, and wherein the security check unit is coupled to receive a current privilege level (CPL) of a task

including the instruction, and wherein the security check logic is configured obtain an additional security attribute of the first memory page from the at least one security attribute data structure, and wherein the security check logic is configured to generate the fault signal [304, fig. 3B; col. 14, line 60 to col. 15, line 5] dependent upon the CPL of the task including the instruction, the additional security attribute of the first memory page, the security attributes of the selected memory page. and the additional security attribute of the selected memory page [col. 3, lines 18-30; col. 4, lines 43-55; col. 13, lines 40-55; col. 17, lines 30-55];

the additional security attribute of the first memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the first memory page is a secure page [col. 14, lines 20-25];

the linear address is produced during execution of an instruction residing within a first memory page [col. 11, line 57 to col. 12, line 5], and wherein the security check unit is coupled to receive a value of a secure execution mode (SEM) bit [e.g., validity check circuit, 304, fig. 3B] indicative of operation in a secure execution mode, and wherein the security check logic is configured obtain an additional security attribute of the first memory page from the at least one security attribute data structure, and wherein the security check logic is configured to generate the fault signal dependent upon the value of the SEM bit, the additional security attribute of the first memory page, the security attributes of the selected memory page, and the additional security attribute of the selected memory page [col. 13, lines 40-55; col. 14, lines 60-67; col. 15, lines 29-45].

the fault signal is a page fault signal as defined by the x86 processor architecture [col. 11, lines 57-60; col. 15, lines 1-5].

4. As per claim 11:

Christie teaches a central processing unit, comprising: an execution unit operably coupled to a memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and a memory management unit (NIMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores data arranged within a plurality of memory pages, and wherein the MMU comprises: a security check unit coupled to receive a physical address within a selected memory page and security attributes of the selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, and to generate a fault signal dependent upon the security attributes of selected memory page and the additional security attribute of the selected memory page [fig. 1, 3A, 3B, 4; abstract; col. 2, lines 27-35; col. 3, lines 20-40; col. 13, lines 39-55; col. 15, lines 29-50].

5. As per claims 12-13:

Claims 12 and 13 are rejected as the same reasons as set forth in claims 1, 7, 9 and 11 due to the same scope.

6. As per claims 14-17:

Christie teaches the paging unit produces the physical address of the selected memory page during execution of an instruction residing within a first memory page; the physical address within the selected memory page includes a base address and an offset; the paging unit is configured to obtain the base address from the at least one paged memory data structure; the at least one paged memory data structure comprises a page directory [privilege level; fig. 3B; user/supervisory mode] and at least one page table as defined by the x86 processor architecture [col. 4, lines 61-65; col. 5, lines 8-35; col. 11, lines 57-65].

7. As per claim 18:

Claim 18 is rejected as the same reasons as set forth in claim 2.

8. As per claims 19-20:

Christie teaches the paging unit is configured to receive security attribute of the instruction and to produce the fault signal dependent upon the security attribute of the instruction and the security attributes of the selected memory page; the security attribute of the instruction comprises a current privilege level (CPL) of a task including the instruction as defined by the x86 processor architecture [col. 15, lines 1-28; col. col. 2, lines 27-35].

9. As per claims 21-22, 24-28:

Claims 21-22, 24-25, 27 are rejected as the same reasons as set forth in claims 9, 3, 5-6.

10. As per claim 29:

Claim 29 is rejected as the same reasons as set forth in claim 10.

11. As per claim 30:

Claim 30 is rejected as the same reasons as set forth in claims 12-13.

12. As per claims 31-33:

Claims 31-33 are rejected as the same reasons as set forth in claims 17, 20, 9.

13. As per claims 34-36:

Claims 34-36 are rejected as the same reasons as set forth in claims 2, 10, 8.

14. As per claims 37-40:

Claims 37-40 are rejected as the same reasons as set forth in claims 6, 22, 23, 24.

15. As per claim 41:

Claim 41 is a method corresponding to the apparatus of claim 30. Therefore, claim 41 is rejected as the same reasons as set forth in claim 30.

16. As per claim 42:

Claim 42 is rejected as the same reasons as set forth in claims 13, 16-17.

17. As per claim 43:

Claim 43 is rejected as the same reasons as set forth in claims 13, 20.

18. As per claim 44:

Claim 44 is rejected as the same reasons as set forth in claims 13, 9.

19. As per claim 45:

Claim 45 is rejected as the same reasons as set forth in claims 13, 2.

20. As per claim 46:

Claim 46 is rejected as the same reasons as set forth in claims 13, 26-29.

21. As per claims 47-48:

Claims 47-48 are rejected as the same reasons as set forth in claims 5-8.

22. As per claim 49:

Claim 49 is rejected as the same reasons as set forth in claims 13, 22.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 23, 29 are rejected under 35 U.S.C 103(a) as being unpatentable over Christie.

23. As per claims 4, 23, 29:

Christie teaches the claimed limitations as noted above.

Christie further teaches the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a

security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory [col. 4, lines 5-60; col. 11, lines 57-65; col. 18, lines 1-3]
Christie implicitly teaches the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry. This is because security check unit protected certain Ranges (secure pages) of non-volatile memory within the Real-Time Clock (RTC) in the Super I/O chip. The protected locations, hereinafter called secure pages, are used to store passwords and other critical information. These secure pages are identified by its base addresses in the security attribute table. Following the boot process, the security check unit in the computer system may not adequately protect the contents of the RTC. For example, an unauthorized user could conceivably modify the base address of the RTC in the security attribute table, and then gain access to unprotected secure locations. The security check unit utilizes base addresses and read/write control signals to the Super I/O chip to prevent access to specific secure pages corresponding to specified logical devices. The security check unit also protects the base address of the secure pages as well as the base addresses of specified logical devices. Protecting the base addresses prevents the security check unit from being circumvented by interfering with the address decoding used to track reads and writes to protected secure pages. Therefore, the first field called the base address field in the security attribute table contained in the super I/O chip must be reserved for base address of those secure pages. This reserved base address field must be protected from unauthorized modification in order to increase the system security.

Conclusion

24. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Stimac et al PN 4,926,322 discloses Paged memory management with privilege levels.
b. Crawford et al PN 5,173,872 discloses privilege levels of security.
c. Anderson PN 5,983,370 discloses security privilege levels, user/supervisory bit.
d. McNabb et al PN 6,289,462 discloses security attribute levels.
e. Kolichtchak Pub. 2003/0014667 discloses user/supervisor and privilege levels.

f. Mckee Pub. 2003/0084256 discloses privilege level-access to memory.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ngoc Dinh whose telephone number is (703) 305-3023. The examiner can normally be reached on Monday-Friday 8:30 AM-5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Donald A. Sparks, can be reached on (703) 308-1756. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

NGOC DINH
Patent Examiner
ART UNIT 2187
March 11, 2004

DONALD SPARKS
Supervisory Patent Examiner
Technology Center 2100